UNITED STATES DISTRICT COURT
FOR THE MIDDLE DISTRICT OF NORTH CAROLINA
CASE NO. 1:20-cv-00954-UA-JLW

FARHAD AZIMA, Plaintiff, v. NICHOLAS DEL ROSSO and VITAL MANAGEMENT SERVICES, INC., Defendants.	)	**SECOND DECLARATION OF VIJAY S. BISHT**

I, **Vijay S. Bisht**, do hereby declare under penalty of perjury pursuant to 28 U.S.C. § 1746 the following:

1. I am a Director of CyberRoot Risk Advisory Private Limited ["**CyberRoot**"]. CyberRoot is a company incorporated under the laws of India that provides risk mitigation, online reputation management, information security, and digital forensics services. Except where otherwise indicated below, this affidavit is based on my personal knowledge, and I believe all facts set forth below to be true.

2. I am over the age of eighteen years of age and competent to testify as to the matters set forth in this Declaration.

3. I previously executed a declaration, dated October 22, 2020, under penalty of perjury relating to my lawful work at CyberRoot, including

CyberRoot's lawful work with its client, Vital Management Services, Inc. A true copy of that declaration is attached hereto as **Exhibit 1**. I reaffirm that the facts contained in that declaration are true. The facts contained in that declaration were true when I executed the declaration, and remain true today.

4. I have been shown a witness statement executed by Mr. Ian Herbert, an attorney at the firm of Miller & Chevalier and submitted in the English Proceedings. A true copy of Mr. Ian Herbert's English Witness Statement is attached hereto as **Exhibit 2** and the exhibit that he filed with his English Witness Statement is attached hereto as **Exhibit 3**. I have also been shown a declaration executed by Mr. Ian Herbert, which includes substantially identical allegations and was contemporaneously filed in this matter, which is attached hereto as **Exhibit 4**. For the purposes of this witness statement, I will refer to Mr. Herbert's allegations in the English witness statement, but my denials apply equally to both submissions by Mr. Herbert. Mr. Herbert alleges that I communicated with him on several occasions, and met face-to-face with him in Tokyo on 20-21 June 2023. I have never met, communicated or had any contact whatsoever with this individual, including in any face-to-face meeting. For the avoidance of doubt, I did not meet with or communicate with Miller & Chevalier as alleged by Mr. Herbert, and I respond below to each of the false allegations made by Mr. Herbert.

5. Mr. Herbert alleges in paragraph 5 of his witness statement that I began text messaging Mr. Kirby Behre, another attorney at the firm of Miller & Chevalier, beginning in February 2023, and offered to provide evidence supporting Mr. Azima's case against Nicholas Del Rosso and Vital. Ex. 2, ¶ 5. Those allegations are false. No such text messages were ever sent by me. On the contrary, and as set forth below and in my October 22, 2020 declaration, I was contacted repeatedly by individuals acting on behalf of Mr. Azima, and threatened that unless I cooperated with them, Miller & Chevalier would sue me on behalf of Mr. Azima.

6. As reflected in my previous declaration, I, and others at CyberRoot, were repeatedly contacted by Mr. Jonas Rey, who advised that he was acting on behalf of Mr. Farhad Azima, and that he urgently needed to talk with me about providing assistance to Mr. Azima. A copy of a WhatsApp message from Mr. Rey is attached to my earlier declaration as Exhibit A. (*See* Ex. 1-A.)

7. The contact by Mr. Rey was followed by a communication from the law firm of Miller & Chevalier, and in particular Mr. Kirby Behre of that firm, on behalf of Mr. Azima, and expressly threatened that Miller & Chevalier and Mr. Kirby would sue CyberRoot if I did not assist Mr. Azima. Ex. 1 ¶¶ 7-25 and Ex.1-B. In order to further pressure me and others at CyberRoot to cooperate with, and assist Mr. Azima, Mr. Behre attached a draft complaint

he claimed that Azima's U.S. counsel – Miller & Chevalier and Womble Bond Dickinson – intended to file against us. A copy of that complaint was attached as Exhibit C to my previous declaration. (*See* Ex. 1-C). Notwithstanding that pressure, I refused to cooperate with Mr. Azima's lawyers because they wanted me to falsely claim that CyberRoot had hacked Mr. Azima's data.

8. Mr. Herbert goes on to allege in his affidavit that after contacting Miller & Chevalier in February 2023, I "repeatedly insisted upon an in-person meeting to provide CyberRoot's information," and further that I "refused to say" what CyberRoot hoped to get out of an in-person meeting." Ex. 2, ¶ 5. As stated above, I had no such communication, and made no such statement, in words or substance to Mr. Herbert, Mr. Behre, or anyone else at Miller & Chevalier.

9. Mr. Herbert then goes on to allege that I subsequently agreed to advise Miller & Chevalier what information CyberRoot could provide, and that Messrs. Herbert and Behre received a text message using an app called "Twinme" in which I admitted several facts which he details in paragraphs 7.1 through 7.7 of his witness statement. Ex. 2, ¶ 7. I have never used Twinme, and was unaware that this messaging application existed until I read Mr. Herbert's witness statement. I do not recognize the messages or username displayed in the messages attached to Mr. Herbert's witness statement. For the avoidance of doubt, I never sent any message using

Twinme or any other means of communication setting forth in words or substance any of the statements contained in Mr. Herbert's witness statement. It is also my understanding and belief that each of the statements alleged by Mr. Herbert to have been made by me are false, and the contents of these purported messages are denied as false.

10. Mr. Herbert then alleges that to prove CyberRoot was involved in hacking Mr. Azima, I provided "passwords of Mr. Azima's that CyberRoot had used to hack Mr. Azima." Ex. 2, ¶ 8. I do not have any such passwords and, in any event, did not provide any such passwords. For the avoidance of doubt, any allegation or suggestion that CyberRoot hacked Mr. Azima is false, and I made no such statement. Throughout CyberRoot's relationship with Vital, I have been the sole point of contact for this client relationship and, for the avoidance of doubt, Vital and Mr. Del Rosso have never requested or instructed that CyberRoot hack Mr. Azima or any other person.

11. Mr. Herbert next claims that I met, along with Mr. Chiranshu Ahuja, "in person on June 20-21, 2023, in Tokyo" with Messrs. Herbert and Behre. Ex. 2, ¶ 10. As with the other allegations, this is false. I did not meet with Messrs. Herbert and Behre in Tokyo, Japan. It would have been impossible for me to have been in Tokyo on those days, as I was in India. A true copy of the receipt of Big Basket, an online grocery store, reflecting a delivery made in my name on 21.06.2023, is attached as **Exhibit 5**.

VSR

Moreover, I have never met with either individual in my life, in Tokyo or elsewhere. It is also false that I made any of the admissions contained in paragraphs 10.1 to 10.7 at such a meeting, and in fact, I never made any of those admissions at any time or place. It is my understanding and belief that each and every alleged "admission" contained in those paragraphs are not true.

12. Not only are the alleged admissions false, in some cases it would have been impossible for them to be true. For instance, Mr. Herbert alleges that Messrs. Neuman and Kelly pressured me to sign my earlier declaration attached as Ex. 2, ¶ 10.7. In fact, my earlier declaration and the declarations of Mr. Vikash Pandey were facilitated by CyberRoot's counsel. CyberRoot's counsel conducted my interview and Mr. Vikash Pandey's interviews, and Messrs. Neuman and Kelly did not attend or participate in our interviews with CyberRoot's counsel. Similarly, I was advised by my own counsel as to the declaration and its contents. Unlike the threats received by Miller & Chevalier when trying to coerce cooperation from me and CyberRoot, I never was pressured by anyone acting on behalf of Mr. Del Rosso or Vital to execute any declaration.

13. In paragraph 11 of his affidavit, Mr. Herbert alleges that I asked to be paid "$20 million in exchange for documentation backing up the information [I and Mr. Ahuja] had already provided." Ex. 2, ¶ 11. No such

statement in words or substance was ever made by me, or to my knowledge, anyone else on behalf of CyberRoot.

14. Mr. Herbert finally alleges that I deleted Signal and Twinme messages after Miller & Chevalier refused our alleged demand for $20 million. Ex. 2, ¶¶ 11-12. As set forth above, no such messages were ever sent by me, or to my knowledge, anyone else at CyberRoot, and neither I nor anyone else, to my knowledge and belief, ever sent or deleted messages sent to Mr. Herbert, Mr. Behre or Miller & Chevalier. I believe that this false allegation was introduced solely to prejudice my ability to respond to Mr. Herbert's false allegations.

15. I declare under penalty of perjury that the foregoing is true and correct pursuant to 28 U.S.C. § 1746.

Executed on July 28, 2023 in Gurugram, Haryana, India.

Vijay S. Bisht

Exhibit 1
(First Declaration of Vijay Bisht)

UNITED STATES DISTRICT COURT
FOR THE MIDDLE DISTRICT OF NORTH CAROLINA
CASE NO. 20-CV-954

FARHAD AZIMA, Plaintiff, v. NICHOLAS DEL ROSSO and VITAL MANAGEMENT SERVICES, INC., Defendants.	)	**DECLARATION OF VIJAY S. BISHT**

I, **VIJAY S. BISHT**, do hereby declare under penalty of perjury pursuant to 28 U.S.C § 1746 the following:

1. I am a Director of CyberRoot Risk Advisory Private Limited ("CyberRoot"). CyberRoot is an Indian company that provides risk mitigation, online reputation management, information security, and digital forensics services.

2. As part of its cybersecurity services, CyberRoot offers ethical security audits of its clients' systems, commonly referred to as "white hat" computer security. CyberRoot does not engage in malicious security breaches, commonly referred to as "black hat" hacking. In addition to providing its services to private clients, CyberRoot also provides services to Public Institutes also.

Initial Contact by Jonas Rey on Behalf of Farhad Azima

3. On October 14, 2020, I was contacted by Jonas Rey by message on WhatsApp, who claimed that he represented Farhad Azima. I did not know Rey, but he

VSB
Initials

introduced himself as being a colleague in the "investigative industry" and he is publicly described as an "ex-Diligence investigator" who founded Athena Intelligence & Risk Management SARL in Switzerland. A true and accurate screen capture of Jonas Rey's initial contact with me by WhatsApp is attached hereto as **Exhibit A**.

4. I did not understand the purpose of Rey's messages to me, and I did not initially take his calls.

5. Rey repeatedly texted me and other Directors of CyberRoot every few hours for three days. I recall that Rey communicated with us exclusively through applications like WhatsApp.

6. I recall that Rey warned me that we could become involved in Azima's complicated dispute but that he could help us find a solution or an easy exit. Rey continued to pressure me and my colleagues at CyberRoot through continuous messages on WhatsApp.

U.S. Counsel for Azima Continue False Accusations and Threats

7. On October 14, 2020, Kirby Behre sent a letter, dated October 13, 2020 to a CyberRoot employee, Vibhor Sharma on behalf of Farhad Azima, which is attached hereto as **Exhibit B**. We also received a draft Complaint on behalf of Farhad Azima, which is attached hereto as **Exhibit C**. I received similar communications from Calvin Lee.

8. The letters and draft "Complaint" falsely accused CyberRoot of being involved in the hacking of Azima. The letter and draft "Complaint" also falsely accused

Initials

Vital Management Services, Inc. ("VMS") and its President, Nicholas del Rosso, of instructing CyberRoot to hack Azima as no such instruction was received by CyberRoot.

9. Neither I nor CyberRoot sent phishing emails to Azima.

10. Neither I nor CyberRoot hacked or otherwise gained unauthorized access to Azima's computer systems. CyberRoot would not accept an engagement for illegal hacking.

11. Neither I nor CyberRoot instructed or assisted any third parties in the alleged hacking of Azima's computer systems. Rather, CyberRoot's business includes protecting our clients' computer systems from malicious attacks.

12. Neither I nor CyberRoot assisted in the dissemination of any allegedly hacked information belonging to Azima.

13. According to the draft Complaint received from Kirby Behre, a company called "BellTroX" is alleged to be responsible for hacking Azima.

14. CyberRoot is not affiliated or connected with, either directly or indirectly, with BellTroX. CyberRoot does not share resources or its employees with BellTroX.

15. The draft Complaint states that Preeti Thapiyal was an employee of BellTroX and CyberRoot. This statement is inaccurate.

16. CyberRoot hired Thapiyal in September 2018 to provide website security audits as part of ongoing projects.

17. I have no knowledge of whether Thapiyal ever worked for BellTroX. During her brief engagement with CyberRoot, Thapiyal requested significant time off to prepare

VSR
Initials

for her wedding, only some of which CyberRoot granted. Thapiyal quit in January 2019. Neither I nor CyberRoot have any knowledge or reason to believe that Thapiyal was involved in the alleged hacking Azima.

18. Neither I nor CyberRoot were instructed by VMS or del Rosso to hack Azima's computer systems. I have no reason to believe that VMS or del Rosso instructed or is otherwise involved in the alleged hacking of Azima's computer systems.

19. VMS is one of CyberRoot's clients and I have worked with VMS throughout our companies' engagement; however, as noted above, neither VMS nor CyberRoot are involved in the alleged hacking of Azima and CyberRoot's engagement was for unrelated matters.

20. CyberRoot has not shared any of its banking or financial records related to VMS with third parties. The draft Complaint appears to rely on financial records that were illegally obtained from either CyberRoot or VMS.

21. CyberRoot and its employees have been harassed by reporters and persons working for Azima since U.S. counsel sent their demand for cooperation to CyberRoot. In particular, a reporter with Thomson Reuters contacted CyberRoot employees and inquired about details that were included in the draft Complaint. Given the timing and detail of the Thomson Reuters inquiries, I reasonably believe that Azima and his representatives coordinated with journalists to increase the reputational harm and pressure on CyberRoot.

22. Since receiving the demand for cooperation from Azima's U.S. counsel, I have learned that other legal representatives of Azima have approached current and former

VSF
Initials

employees of CyberRoot and have pressured them to provide false statements implicating CyberRoot and others in the alleged hacking of Azima.

23. For example, in August and September 2020, Burlingtons Legal LLP ("Burlingtons") attempted to pressure Vikash Pandey into signing documents that falsely implicated CyberRoot and others in the alleged hacking of Azima's computer systems. I understand that Pandey was threatened with criminal and legal proceedings and that Pandey was also offered considerable compensation if he was willing to provide statements of his involvement, which he had already denied.

24. I also understand and believe that Azima and his representatives have approached other current and former employees of CyberRoot with similar threats of criminal penalties and offers of payment for statements that would falsely implicate CyberRoot or others in the alleged hacking of Azima.

25. Based on similar demands from Azima's U.S. counsel that CyberRoot implicate others to avoid U.S. criminal penalties, I reasonably believe that Azima intended to obtain false confessions from CyberRoot.

26. I declare under penalty of perjury that the foregoing is true and correct.

Executed on October 22, 2020 in Dehli, India.

Vijay S. Bisht

Initials

Exhibit A

15:31 23%

+41 79 944 95 71

TODAY

Messages and calls are end-to-end encrypted. No one outside of this chat, not even WhatsApp, can read or listen to them. Tap to learn more.

Dear Vijay, my name is Jonas and there is something I need to discuss with you urgently. Would you be available for a brief call today? 13:10

Missed voice call at 15:12

Hi, do I know you? 15:19

Hi, no but i'm a colleague from the investigative industry. Its important we can connect. I represent Mr. Farhad Azima, who wants me to pass on a document to you and to Vibhor Sharma. It's important we can speak about it. 15:22

I don't understand your concern and which document you are talking about? 15:26

Before I send it over here could you just confirm you are indeed Vijay Bisht? The document is confidential and meant only for the directors of CyberRoot 15:28

Type a message

Exhibit B

Kirby Behre
Member
(202) 626-5960
kbehre@milchev.com

October 13, 2020

CONFIDENTIAL
OFFER OF SETTLEMENT UNDER FRE 408
WITHOUT PREJUDICE

Via E-mail

Vibhor Sharma
House Number-791, 10a, Sector Rd,
IOC Colony, Sector 10A,
Gurugram, Haryana 122003, India

Re: Your Involvement in the Hacking of Farhad Azima

Dear Mr. Sharma:

We represent Farhad Azima regarding the hacking he suffered. We have learned that you and CyberRoot Risk Advisory Private Limited were directly involved in the hacking of Mr. Azima and the distribution of his stolen data, and that CyberRoot was paid more than $1 million to steal Mr. Azima's data on behalf of RAKIA. Mr. Azima intends to file suit against you and CyberRoot, and we write before doing so to offer you the opportunity to cooperate with us regarding this matter.

The attached draft complaint summarizes some, but not all, of the misconduct you and others were involved in relating to the hacking of Mr. Azima. Any complaint we file may include additional allegations, and similar lawsuits may be filed in other jurisdictions, including the UK. However, if you are willing to cooperate fully with us in recovering damages from those involved, we will consider releasing you from Mr. Azima's claims in all jurisdictions.

Your truthful cooperation will not be valuable to us if you disclose the attached draft complaint, this letter, or any information regarding our offer of settlement with anyone other than a lawyer if you choose to consult with one. If we reach an agreement regarding your cooperation, we will ask that you confirm to us in writing that you (and any lawyer you retain, if you decide to retain one) have not shared this information with anyone.

If you are interested in discussing the possibility of cooperating with us, we must hear from you before 5 pm Eastern time on Thursday, October 15, 2020. Should you decide not to cooperate, our client will proceed to file suit without further notice.

Sincerely,

Kirby Behre

cc: Ian Herbert, Miller & Chevalier Chartered
Chris Jones, Womble Bond Dickinson
Ripley Rand, Womble Bond Dickinson

Enclosure

Exhibit C

UNITED STATES DISTRICT COURT
FOR THE MIDDLE DISTRICT OF NORTH CAROLINA

FARHAD AZIMA, 5921 Ward Parkway Kansas City, Missouri 64113, Plaintiff, v. CYBERROOT RISK ADVISORY PRIVATE LIMITED, VIBHOR SHARMA, Defendants.	)	Civil Action No. XXXXXX

COMPLAINT

1. Plaintiff, Farhad Azima, by and through his undersigned counsel, files this Complaint against CyberRoot Risk Advisory Private Limited ("CyberRoot") and Vibhor Sharma ("Sharma") and alleges as follows:

INTRODUCTION

2. Over the course of more than two years, Defendants conducted a prolonged hacking of Plaintiff Farhad Azima and stole Azima's computer data, including emails and trade secrets. The stolen data was then published online and used by Defendants and others, on behalf of the Ras Al Khaimah Investment Authority ("RAKIA"), in order to ruin Azima's reputation and damage him financially.

3. Defendants conspired and coordinated with Vital Management Services Inc. ("Vital"), and its owner and sole employee Nicholas Del Rosso. Upon information and belief,

Vital and Del Rosso were engaged and paid by Dechert LLP LLP, which represented RAKIA in a dispute with Azima.

4. RAKIA, the state investment entity for the government of Ras Al Khaimah, hired individuals and companies, directly and through Dechert LLP, to investigate Azima, hack his computers, steal his private data, and weaponize that data to ruin Azima. Those individuals and companies included Stuart Page in the United Kingdom and Del Rosso and Vital in the United States. Del Rosso and Vital hired Defendants to carry out the hacking of Azima.

5. Defendant CyberRoot is located in Gurgaon, India and engages in illegal hacking. Defendant Sharma is a director of CyberRoot.

6. BellTroX Info Tech Services ("BellTroX") assisted Defendants in hacking Azima. BellTroX is a hacking company based in New Delhi, India. According to a June 9, 2020 Thomson Reuters press report, BellTroX was involved in "one of the largest spy-for-hire operations ever exposed," helping clients spy on more than 10,000 email accounts over a period of seven years. On February 11, 2015, the founder and owner of BellTroX, Sumit Gupta, was indicted by the United States Department of Justice in the Northern District of California for hacking. Mr. Gupta remains at large.

7. In its investigation of 'hack-for-hire' organizations (including BellTroX), Thomson Reuters reviewed a cache of data revealing "tens of thousands of malicious messages designed to trick victims into giving up their passwords" – phishing and spear phishing emails – that BellTroX distributed between 2013 and 2020. Upon information and belief, the data cache revealed that email accounts belonging to Azima and his associates were among the accounts targeted by the BellTroX/CyberRoot phishing operation.

8. Defendants sent Azima phishing and spear-phishing emails and successfully induced Azima to unwittingly provide them with passwords for his accounts. The successful hack gave Defendants persistent access to Azima's computers and email accounts, and Defendants obtained real-time access to Azima's emails. Defendants disclosed Azima's stolen data on internet blog sites they created. Those blog sites contained links to BitTorrent sites and WeTransfer sites, set up by the Defendants, that contained substantial quantities of Azima's stolen data.

9. Defendants were paid more than $1 million for the hacking of Azima and dissemination of his stolen data. The work done by Defendants, assisted by Bell TroX, was paid for and done at the direction of the Del Rosso, Vital, and others.

10. Defendants hacked Azima because they were hired to do so on behalf of RAKIA by Del Rosso and Vital, who were hired by Dechert LLP and partner Neil Gerrard. Dechert LLP represented RAKIA in a dispute with Azima, and Gerrard wanted Azima's stolen data to use in a suit to be brought by RAKIA against Azima in England. Page, Del Rosso, Gerrard, and RAKIA's manager James Buchanan created a false evidentiary trail to cover up their and RAKIA's responsibility for the hacking, and to suggest that Page had innocently found the hacked material on BitTorrents. RAKIA brought the lawsuit against Azima using the hacked material. The hacking was a defense raised by Azima, as well as forming the basis for a counterclaim by Azima.

11. Following a January 2020 trial in the U.K., the English court ruled that RAKIA, Page, and others had lied about how they obtained Azima's stolen data. Del Rosso, who paid the Defendants to hack Azima, gave a sworn witness statement and sworn trial testimony denying any knowledge of how the stolen emails were obtained. The sworn witness statement and sworn testimony were both false. Defendants and others hacked Azima at the direction of Vital, Del Rosso, and others, and provided Azima's stolen data directly to Vital and Del Rosso to be used by

Dechert LLP against Azima. RAKIA's lawyers, including Dechert LLP, had also asserted (in formal correspondence, witness evidence and pleadings signed by those lawyers) that RAKIA had innocently discovered the materials on the internet. Those assertions were also false, given the Judge's ruling.

12. As a result of the conduct of CyberRoot, Sharma, and their co-conspirators, Azima has suffered significant financial and reputational damage.

PARTIES

13. Plaintiff Azima is a U.S. citizen who resides and works in Kansas City, Missouri. He is a successful businessman who has owned and operated multiple aviation-related companies. Azima's businesses engage in interstate and foreign commerce. All of Azima's computers and servers were and are located in the United States.

14. Defendant CyberRoot is a limited company incorporated under the laws of India (registration number 50078) with its registered address at House Number-791, 10a, Sector Rd, IOC Colony, Sector 10A, Gurugram, Haryana 122003, India. CyberRoot is a cybersecurity actor and investigation firm. In its original Memorandum of Association, an object of CyberRoot was stated to be "to carry on the business of … hacking."

15. Defendant Sharma is a director of CyberRoot and has been since 2 May 2014.

16. Vital is a one-man private investigation company. Del Rosso is the owner and sole employee of Vital. Del Rosso is the president and owner of Vital, and he is one of two shareholders of Vital, along with his wife. Vital and Del Rosso are both located in North Carolina.

FACTS

Hacking of Azima

17. Starting in early 2015, Gerrard, Page, Buchanan, and others agreed to attack Azima. The agreement is evidenced by a redacted internal "Project Update" report dated March 26, 2015,

presented by Page to the Ruler of RAK and provided to Buchanan and others, as well as numerous emails between Gerrard, Buchanan, and their associates, some of which discussed the plan to "target," "attack," and "go after" Azima using "another channel." Based on these emails, an English court concluded that the desire to attack Azima in the summer of 2015 "is clear." The Project Update report claimed Azima was part of a "US team" to publicize human rights abuses by RAK and Gerrard. The report stated that "The campaign is not public yet, so we will be able to gather intelligence on their progress in order to monitor their activities and attempt to contain or ruin their plans." Gerrard admitted to reading this report.

18. Gerrard hired Del Rosso and Vital. Upon information and belief, Del Rosso was hired to target Azima and to obtain Azima's emails and confidential data, and for other purposes; and Page was retained to assist in the targeting of Azima, which upon information and belief included hacking Azima. Del Rosso hired the Defendants to lure Azima into providing his login data, so that Defendants and their co-conspirators could have persistent access to Azima's accounts and computers.

19. At least five employees of CyberRoot, including Sharma, hacked Azima pursuant to Del Rosso's instructions. CyberRoot was assisted by BellTroX, which permitted Defendants to use BellTroX's infrastructure, including its server, to hack Azima and Massaad at the direction of Del Rosso and others. Cyberroot and BellTroX also share common employees. One such employee is Mr Preeti Thapiyal whose LinkedIn page lists his work as including the creation of "undetectable phishing Payloads."

20. Defendants, assisted by BellTroX, attempted to gain access to Azima's computers and accounts through phishing and spear-phishing emails. They sent Azima phishing emails to harvest his credential and gain access to his email accounts and computers. Azima complied, and

unwittingly enabled Defendants to gain access to Azima's email accounts and computers. The breach of Azima's computer systems gave Defendants covert and persistent access to Azima's email accounts and computers. Defendants also successfully hacked Forsan Ceramics, a company of Massaad's that is based in Saudi Arabia.

21. Defendants, Del Rosso, Vital, and other co-conspirators, including Dechert LLP, Gerrard, and Page, obtained numerous confidential and protected trade secrets belonging to Azima and his companies, including but not limited to privileged and confidential legal communications and advice and confidential internal pricing lists relating to food transport for U.S. troops in Afghanistan.

Disclosure of Azima's Data

22. Defendants created, uploaded, and transmitted multiple unauthorized copies of Azima's data. Upon information and belief, some of that data was provided to Del Rosso, who was located in the United States.

23. In late July 2016, Gerrard met with Azima and threatened him. Within days of Gerrard's meeting with Azima, on or about August 7, 2016, Defendants created blog sites accusing Azima of fraud. The blog sites contained links to BitTorrent sites that Dechert LLP later admitted contained large quantities of Azima's stolen data. These BitTorrent links were posted by users named anjames and an_james, which are usernames associated with Sharma at CyberRoot. Defendants also used the email account an_james@protonmail.ch to create these blog sites and upload Azima's stolen data. During this same period, Del Rosso made significant payments to Defendants for their efforts.

24. Defendants posted the data on the internet to create the misimpression that the data they stole from Azima were available to anyone who used the internet. Defendants created

BitTorrent links that contained Azima's stolen data and those links were posted on the blog sites alleging fraud by Azima. Page, Del Rosso, Gerrard, and an Israeli journalist, Majdi Halabi, created a false story and evidentiary trail to cover up their and RAKIA's responsibility for the hacking, and to suggest that Page had innocently found the hacked material on BitTorrents after being alerted to it by Halabi.

25. In fact, the data on the BitTorrent links were not accessible to the public because the 'seeders'[1] necessary for the data to be downloaded were not available. Dechert LLP, and others acting at their direction, are the only persons or entities known to have obtained the data from the BitTorrent sites.

26. In May and June 2018, the blog sites were modified to include new links to WeTransfer sites that contained copies of Azima's stolen data.

27. Defendants regularly used WeTransfer links to transfer data to Vital. Defendants set up the WeTransfer account using the email account an_james@protonmail.ch.

28. In June 2019, the links on the blog sites were modified to include new WeTransfer links containing some of Azima's stolen data. These links, as with all the links to copies of Azima's stolen data, were not authorized by Azima.

29. Del Rosso and Vital paid Defendants more than $1 million for their hacking services and the distribution of Azima's stolen data. The payments were made by Del Rosso and Vital to CyberRoot's bank, Kotak Mahindra Bank. Substantial payments were made to CyberRoot around the time that Azima's stolen data was published online.

JURISDICTION

[1] A torrent seeder is a user who owns the file being made available online through the torrent system. Without a seeder, a file cannot be downloaded.

30. This Court has federal question subject matter jurisdiction pursuant to 28 U.S.C. § 1331. Some of Azima's claims arise under federal law, including the Wiretap Act (Counts 1 and 2) and misappropriation of trade secrets under the Defend Trade Secrets Act and the Economic Espionage Act (Count 3).

31. The Court has supplemental jurisdiction pursuant to 28 U.S.C. § 1367 over Azima's other claims, since those other claims relate to the federal statutory claims in this action and form part of the same case or controversy under Article III of the United States Constitution.

32. Additionally, this Court has diversity subject matter jurisdiction pursuant to 28 U.S.C. § 1332 because Azima and Defendants are from different states and the amount in controversy exceeds $75,000, exclusive of interest and costs.

33. Under North Carolina common law, co-conspirators have sufficient connections to the forum state for personal jurisdiction where "substantial acts in furtherance of the conspiracy were performed in the forum state and the co-conspirator knew or should have known that acts would be performed in the forum state." *Gemini Enterprises, Inc. v. WFMY Television Corp.*, 470 F.Supp. 559, 562-565 (M.D.N.C. 1979). Defendants Sharma and CyberRoot plotted substantial acts in furtherance of the conspiracy against Azima with Del Rosso and Vital, both of which are based in North Carolina. Del Rosso and Vital paid Defendants Sharma and CyberRoot more than $1 million to carry out the conspiracy to hack Azima. Upon information and belief, those payments went through a North Carolina bank, and the instructions to pay Defendants came from Del Rosso and Vital in North Carolina.

34. The Court's jurisdiction over Defendants comports with due process. The Court has personal jurisdiction over Defendants Sharma and Cyberroot, who have conspired with North Carolina residents Del Rosso, Vital, and others to harm Azima. From North Carolina, Del Rosso

and Vital hired Sharma and Cyberroot to launch a computer hack of Azima, in furtherance of the conspiracy to retaliate against and discredit Azima.

VENUE

35. Venue is proper under 18 U.S.C. § 1965(a) because the Defendants transact their affairs in this Judicial District. Defendants Sharma and Cyberroot both received instructions and payments in U.S. dollars from Chapel Hill, North Carolina, with Azima's causes of action arising out of those North Carolina transactions.

36. Venue is also proper under 28 U.S.C. § 1391(b)(2) because this is a judicial district in which a substantial part of the events or omissions giving rise to the claim occurred. Defendants Sharma and Cyberroot conspired with Del Rosso, Vital, and others in Chapel Hill, North Carolina to coordinate their illegal campaign to hack Azima and publish his stolen data.

37. Venue is also proper under 28 U.S.C. § 1391(b)(3) because this judicial district has personal jurisdiction over all defendants.

COUNT ONE (All Defendants)

I. Disclosure of Wire, Oral, or Electronic Communications under the Wiretap Act (18 U.S.C. §§ 2511(1)(c) and 2520)

38. Plaintiff incorporates by reference the allegations contained in the preceding paragraphs.

39. Under 18 U.S.C. § 2511(c), any person who "intentionally discloses, or endeavors to disclose, to any other person the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication."

40. "Intercept" is defined as "the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device." 18 U.S.C. § 2510(4).

41. "Electronic communication" means any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic, or photooptical system that affects interstate or foreign commerce."

42. In violation of 18 U.S.C. § 2511(1)(c), Defendants CyberRoot and Sharma intentionally disclosed wire and electronic communications of Azima knowing and/or having reason to know that the information was obtained through interception.

43. In coordination with Del Rosso, Vital, and others, Defendants intentionally disclosed large quantities of Azima's intercepted data on BitTorrent and WeTransfer. Links to those BitTorrent and WeTransfer sites were added to the blog sites Defendants created. Cyber Root worked with Bell Trox to conduct the hacking and post the intercepted data. The intercepted data included, among other things, business and personal electronic communications between Azima and others across the United States and around the world.

44. In 2015, Defendants hacked Azima's computers and email accounts through phishing and spear-phishing emails. The hack gave Defendants persistent access to Azima's computers and email accounts.

45. After Gerrard threatened Azima in 2016, Defendants disclosed Azima's stolen data online. Defendants created multiple websites accusing Azima of fraud. On those websites, Defendants published Azima's stolen data through BitTorrent and WeTransfer links. The BitTorrent and WeTransfer links were posted by users named anjames and an_james, which are

usernames associated with Sharma at CyberRoot. Defendants also used the email account an_james@protonmail.ch to create these blog sites and upload Azima's stolen data. The links were updated as recently as 2019.

46. Defendants had reason to know that the information was obtained through interception because Defendants intercepted Azima's data. The hacking of Azima's data resulted in persistent access to Azima's computers and email accounts.

47. As a result of the disclosure of Azima's intercepted data, Azima suffered damages. Since at least June 2018, the stolen data has continued to be publicly available on WeTransfer through links that were posted to the blog sites created by the Defendants, resulting in more than $75,000 of statutory damages under 18 U.S.C. § 2520(c)(2)(B), and further monetary damages in an amount to be proven at trial. Defendants have made significant profits from the disclosure of Azima's data, having been paid large sums of money to disclose the stolen data to damage Azima. As a result of the continued disclosure of Azima's stolen data, Azima has suffered, and will continue to suffer, irreparable harm to his person, reputation, business, and community standing.

COUNT TWO (all Defendants)

II. Conspiracy to Disclose and Use Intercepted Wire, Oral, or Electronic Communications under the Wiretap Act (18 U.S.C. §§ 2511(1)(d) and 2520, 18 U.S.C. § 371)

48. Plaintiff incorporates by reference the allegations contained in the preceding paragraphs.

49. Defendants willfully, intentionally, and knowingly agreed and conspired with Del Rosso, Vital, and others to disclose Azima's intercepted data in violation of 18 U.S.C. §§ 2511 and 2520. Among other things, Defendants agreed and conspired with Del Rosso, Vital, and others

to intercept Azima's data through a phishing and spear-phishing campaign resulting in the Defendants obtaining persistent access to Azima's computers and email accounts. Defendants also agreed and conspired with Del Rosso, Vital, and others to disclose the intercepted data. Del Rosso, Vital, and others instructed Defendants to publish the data on blog sites that were created by Defendants. Defendant used BitTorrent and WeTransfer to send the stolen data to Defendants Del Rosso and Vital, as well as other co-conspirators. The BitTorrent and WeTransfer links were posted by users named anjames and an_james, which are usernames associated with Sharma at CyberRoot. Defendants also used the email account an_james@protonmail.ch to create these blog sites and upload Azima's stolen data. The links were updated as recently as 2019. Del Rosso and Vital paid Defendants more than $1 million for the interception and publication of Azima's data.

50. Defendants, with full knowledge that they were engaged in wrongful actions, took steps in furtherance of the conspiracy, including receiving more than $1 million from Del Rosso to conduct the hacking.

51. Azima has been injured and has suffered monetary damages as a result of Defendants' conspiratorial actions in an amount to be proven at trial. As a result of the Defendant's conspiracy to disclose and use Azima's intercepted data, Azima has suffered, and will continue to suffer, irreparable harm to his person, reputation, business, and community standing.

COUNT THREE (All Defendants)

III. Misappropriation of Trade Secrets, 18 U.S.C. §§ 1831, 1832, 1836

52. Plaintiff incorporates by reference the allegations contained in the preceding paragraphs.

53. Federal law creates a cause of action against "[w]hoever, with intent to convert a trade secret, that is related to a product or service used in or intended for use in interstate or foreign

commerce, to the economic benefit of anyone other than the owner thereof, and intending or knowing that the offense will, injure any owner of that trade secret, knowingly . . . steals, or without authorization appropriates, takes, carries away, or conceals, or by fraud, artifice, or deception obtains" trade secrets. 18 U.S.C. § 1832(a)(1).

54. Federal law imposes criminal penalties on "whoever . . . conspires with one or more other persons" to violate § 1832(a)(1). See § 1832(a)(5).

55. Federal law also creates a cause of action against "[w]hoever, intending or knowing that the offense will benefit any foreign government, foreign instrumentality, or foreign agent, knowingly – (1) steals, or without authorization appropriates, takes, carries away, or conceals, or by fraud, artifice, or deception obtains a trade secret." 18 U.S.C. § 1831(a)(1).

56. Federal law imposes penalties on "[w]hoever . . . conspires with one or more other persons to commit" the offense listed in § 1831(a)(1). See § 1831(a)(5).

57. "An owner of a trade secret that is misappropriated may bring a civil action . . . if the trade secret is related to a product or service used in, or intended for use in, interstate or foreign commerce." 18 U.S.C. § 1836(b)(1).

58. Azima's email accounts stored secrets including but not limited to highly confidential business plans and proposals, research supporting those plans and proposals including costs and service projections, information concerning business strategies and opportunities, and contacts for important business relationships. These trade secrets are substantially valuable to Azima, in excess of $75,000, as will be proven at trial.

59. Azima stored trade secrets that were used in interstate and foreign commerce. Azima has taken and continues to take reasonable measures to keep this information secret. For

example, Azima has always maintained his information on secured servers that are protected by passwords, firewalls, and antivirus software.

60. Azima's trade secrets drive independent actual and potential economic value from being generally known or available to the public or other persons who can obtain economic value from their disclosure or use.

61. Azima's trade secrets have significant value, resulting from substantial investment of time and resources.

62. Azima has made, and continues to make, efforts that are reasonable under the circumstances to maintain the secrecy of his trade secrets.

63. Defendants, along with other co-conspirators, unlawfully conspired with Del Rosso, Vital, and others to take, appropriate, and obtain Azima's trade secrets without authorization, by means of a cyberattack against him. Defendants and their co-conspirators knew that Azima's email accounts contained trade secrets and intended to steal them in order to harm Azima.

64. Defendants improperly disclosed and misappropriated Azima's trade secrets without consent or authorization when acted on instructions to hack Azima, steal copies of his data, including trade secrets, and distribute the data through BitTorrent and WeTransfer links on blogs created by CyberRoot.

65. As a direct consequence of the unlawful actions of Defendants and their co-conspirators, Azima has suffered damages, which include, but are not limited to, loss of business goodwill, loss in the value of his trade secrets and confidential business information, and harm to Azima's business, in an amount to be proven at trial. *See* 18 U.S.C. § 1836(b)(3)(B)(i)(I). Defendants' acts of misappropriation have affected interstate commerce.

66. As a direct consequence of the unlawful actions of Defendants and their co-conspirators, Defendants have unjustly benefited from their possession of Azima's trade secrets. Defendants were paid more than $1 million to hack Azima, steal his data, including his trade secrets, and publish his stolen data.

67. Defendants' conduct was willful and malicious.

COUNT FOUR (All Defendants)

IV. Computer Trespass (N.C. Gen. Stat. § 14-458)

68. Plaintiff incorporates by reference the allegations contained in the preceding paragraphs.

69. In violation of N.C. Gen. Stat § 14-458, Defendants knowingly and without authorization or reasonable grounds used Azima's computer and computer network with the intent to make or cause to be made unauthorized copies of Plaintiff's computer data.

70. Defendants conspired with others to use Azima's computer and computer network without authorization to make copies of Plaintiff's trade secrets, confidential business information, and personal information and communications that would provide leverage over Plaintiff.

71. Del Rosso, Vital, and others instructed Defendants to hack Azima's computer and computer network. Defendants, which was assisted by BellTroX, carried out the hack on Azima and gained access to Azima's computer and computer network. The breach of Azima's computer systems gave Defendants persistent access to Azima's email accounts and computers. Thus Defendants, acting at the direction of Del Rosso, Vital, and others, regularly used Azima's computer and computer networks to make unauthorized copies of Azima's computer data. Del Rosso and Vital paid Defendants more than $1 million for their hacking services.

COUNT FIVE (All Defendants)

V. Conversion

72. Plaintiff incorporates by reference the allegations contained in the preceding paragraphs.

73. Defendants directly and/or through their agents, knowingly and without authorization or reasonable grounds, wrongfully possessed and converted computer data, documents, spreadsheets, communications, and other files owned by the Plaintiff.

74. Under North Carolina law, conversion occurs when a defendant wrongfully possesses or converts property under the ownership of the Plaintiff.

75. Defendants conspired to wrongfully obtain possession of Plaintiff's computer data, documents, spreadsheets, communications, and other files owned by the Plaintiff.

76. As discussed in more detail above, Del Rosso, Vital, and others instructed Defendants to hack Azima and make unauthorized copies of Azima's computer data. At the direction of Del Rosso, Vital, and others, Defendants successfully hacked Azima and obtained persistent access to Azima's email accounts and computers. Thus Defendants, acting at the direction of Del Rosso, Vital, and others, regularly used Azima's computer and computer networks to make unauthorized copies of Azima's computer data. Del Rosso and Vital paid Defendants more than $1 million for their hacking services.

COUNT SIX (All Defendants)

VI. Identity Theft (N.C. Gen. Stat. § 14-113.20 and § 1-539.2(c))

77. Plaintiff incorporates by reference the allegations contained in the preceding paragraphs.

78. Defendants knowingly and without authorization or reasonable grounds, obtained, possessed, and used identifying information of Plaintiff with the intent to fraudulently represent

that Defendants were the Plaintiff for the purposes of obtaining materials of value, benefit, and advantage.

79. Pursuant to N.C. Gen. Stat. § 14-113.20, "identifying information" is defined to include "passwords;" "electronic identification numbers, electronic mail names or addresses, Internet account numbers, or Internet identification names;" and "any other numbers or information that can be used to access a person's financial resources."

80. Defendants conspired with Del Rosso, Vital, and others to obtain, possess, and use Plaintiff's identifying information – including electronic mail passwords – for the purposes of obtaining trade secrets, confidential business information, and personal information and communications that would provide leverage over Plaintiff.

81. At the direction of Del Rosso, Vital, and others, Defendants sent Azima phishing emails asking him to reset his password. Azima complied, and unwittingly permitted Defendants to gain access to Azima's email accounts and computers. The persistent access to Azima's email accounts and computers allowed Defendants, at the direction of Del Rosso, Vital, and others, to use Azima's email addresses and passwords to obtain substantial quantities of Azima's private data, including trade secrets, confidential business information, and personal information and communications.

COUNT SEVEN (All Defendants)

VII. Publication of Personal Information (N.C. Gen. Stat. § 75-66)

82. Plaintiff incorporates by reference the allegations contained in the preceding paragraphs.

83. Defendants knowingly broadcast or published personal information of Azima's over the internet with actual knowledge that Azima objected to any such disclosure and without Azima's consent or knowledge.

84. Defendants published Azima's private information on blog sites hosting WeTransfer links in May and June of 2018, and again in June of 2019.

85. This personal information included, among others, checking account numbers, passwords, and other numbers and information that can be used to access Azima's financial resources.

86. Among other documents, Defendants published financial transaction records, spreadsheets, business records, and banking information – all marked confidential.

87. Defendants' publication of Azima's personal information on the internet despite Azima's objection and without Azima's consent or knowledge directly and proximately caused actual injury to Plaintiff.

88. Azima is entitled to damages for each of Defendants' unlawful acts of publication of personal information in accordance with N.C. Gen. Stat. § 1-539.2(c).

COUNT EIGHT (All Defendants)

VIII. Violation of Trade Secrets Protection Act (N.C. Gen. Stat. § 66-153)

89. Plaintiff incorporates by reference the allegations contained in the preceding paragraphs.

90. Azima's email accounts and computer systems contained business or technical information, formulas, patterns, programs, devices, compilations of information, methods, techniques, or processes. This information included highly confidential business plans and proposals, research supporting those plans and proposals (including costs and service projections),

information concerning business strategies and opportunities, and contacts for important business relationships. This information constituted trade secrets under Chapter 66 of the North Carolina General Statutes.

91. Azima derived independent actual or potential commercial value from these trade secrets not being generally known or readily ascertainable through independent development or reverse engineering by persons who can obtain economic value from their disclosure or use.

92. Azima has undertaken and continues to undertake reasonable efforts under the circumstances to maintain the secrecy of his trade secrets. For example, Plaintiff has always maintained his information on secured servers that are protected by passwords, firewalls, and antivirus software.

93. Azima's trade secrets are substantially valuable to Plaintiff, in excess of $75,000, as will be proven at trial.

94. Azima kept trade secrets that were used in interstate and foreign commerce.

95. Azima's trade secrets have significant value, resulting from substantial investment of time and resources. If known to Azima's competitors, Plaintiff's trade secrets would be of value to those competitors.

96. Azima's trade secrets included, among others, confidential internal price lists and confidential spreadsheets connected to contracts with the United States government to supply troops in Afghanistan.

97. Defendants Sharma and CyberRoot, along with Del Rosso, Vital, Dechert LLP, Page, and others, unlawfully conspired to acquire, disclose, or use Azima's trade secrets without express or implied authority or consent by means of a cyberattack against Azima. Defendants Sharma and CyberRoot and their co-conspirators knew that Azima's email accounts and computer systems

contained trade secrets and intended to steal them in order to harm Azima. Defendants did not arrive at Azima's trade secrets by means of independent development, reverse engineering, or by obtaining them from a person or entity with a right to disclose any of the trade secrets.

98. Defendants Sharma and CyberRoot improperly acquired, disclosed, or used Azima's trade secrets without consent or authorization when they hacked Azima, steal copies of his data, including trade secrets, and distribute the data through BitTorrent and WeTransfer links on blogs Defendants created.

99. Defendants' conduct in acquiring, disclosing, or using Azima's trade secrets was willful and malicious and part of a deliberate, clandestine strategy to injure Azima.

100. Azima discovered that Defendants misappropriated his trade secrets on or about (date after an investigation that began after revelations at the UK trial, etc.).

101. As a direct consequence of the unlawful actions of Defendants Sharma and CyberRoot and their co-conspirators, Azima has suffered damages, including but are not limited to loss of business goodwill, loss in the value of his trade secrets and confidential business information, and harm to Azima's business, in an amount to be proven at trial. Defendants' acts of misappropriation have affected interstate commerce.

102. As a direct consequence of the unlawful actions of Defendants Sharma and CyberRoot, and their co-conspirators, Defendants Sharma and CyberRoot have unjustly benefited from their possession of Azima's trade secrets. Upon information and belief, Defendants Sharma and CyberRoot, who were engaged by Dechert LLP through Del Rosso and Vital, were paid substantial sums of money by Dechert LLP to conspire to misappropriate Azima's trade secrets.

103. Defendants' conduct in misappropriating Azima's trade secrets as described above directly and proximately caused actual injury to Azima.

104. Because Defendants' conduct was willful and malicious, Azima is entitled to punitive damages pursuant to N.C. Gen. Stat. § 66-154(c).

105. Because Defendants' conduct was willful and malicious, Azima is entitled to reasonable attorney's fees under N.C. Gen. Stat. § 66-154(d).

COUNT NINE (All Defendants)

IX. Unfair and Deceptive Trade Practices (N.C. Gen. Stat. § 75-1.1)

106. Plaintiff incorporates by reference the allegations contained in the preceding paragraphs.

107. Defendants' conduct in sending Azima phishing and spear phishing emails in an effort to access his emails, computers, communications, confidential information, personal information, trade secrets, and other data constitutes an unfair and deceptive act or practice in violation of N.C. Gen. Stat. § 75-1.1.

108. Defendants' conduct in accessing Azima's emails, computers, communications, confidential information, personal information, trade secrets, and other data without his consent or knowledge constitutes an unfair and deceptive act or practice in violation of N.C. Gen. Stat. § 75-1.1.

109. Defendants' conduct in publishing or distributing Azima's emails, communications, confidential information, personal information, trade secrets, and other data on the internet constitutes an unfair and deceptive act or practice in violation of N.C. Gen. Stat. § 75-1.1.

110. Defendants committed conduct in or affecting commerce by (1) sending Azima phishing and spear phishing emails, (2) accessing Azima's emails, computers, communications, confidential information, personal information, trade secrets, and other data without his consent or

knowledge, and (3) publishing or distributing Azima's emails, communications, confidential information, personal information, trade secrets, and other data on the internet.

111. Defendants committed conduct that was unfair and deceptive by (1) sending Azima phishing and spear phishing emails, (2) accessing Azima's emails, computers, communications, confidential information, personal information, trade secrets, and other data, and (3) publishing Azima's emails, communications, confidential information, personal information, trade secrets, and other data on the internet.

112. Defendants' conduct in committing the unfair and deceptive acts or practices as described above was willful and malicious and part of a deliberate, clandestine strategy to injure Azima.

113. Defendants' conduct in committing the unfair and deceptive acts or practices as described above directly and proximately caused actual injury to Azima.

114. Plaintiff discovered that Defendants committed unfair and deceptive acts or practices that injured him on or about August 28, 2020 following an investigation.

115. Because Defendants' conduct constituted unfair and deceptive acts or practices under N.C. Gen. Stat. § 75-1.1, Plaintiff's damages should be trebled pursuant to N.C. Gen. Stat. § 75-16.

116. Because Defendants' conduct constituted unfair and deceptive acts or practices under N.C. Gen. Stat. § 75-1.1 and Defendants willfully and maliciously engaged in that conduct, Plaintiff is entitled to recover reasonable attorney's fees pursuant to N.C. Gen. Stat. § 75-16.1.

COUNT TEN (All Defendants)

X. Civil Conspiracy (North Carolina Common Law)

117. Plaintiff incorporates by reference the allegations contained in the preceding paragraphs.

118. Defendants knowingly and without authorization or reasonable grounds, wrongfully entered an agreement to commit unlawful acts resulting in injury to Azima by conspirators pursuant to a common scheme of stealing Azima's confidential information to use against him.

119. Under North Carolina law, a civil conspiracy occurs when there is an agreement between two or more individuals to do an unlawful act or to do a lawful act in an unlawful way, resulting in injury to a plaintiff inflicted by one or more of the conspirators pursuant to a common scheme.

120. Defendants entered into an agreement with Del Rosso, Vital, and others.

121. Under this agreement, Defendants would send phishing emails to induce Azima to reveal his passwords. Defendants would then use Azima's passwords to gain access to Azima's confidential information and copy the information for widespread publication. Del Rosso and Vital paid Defendants more than $1 million for these actions. Upon information and belief, Del Rosso and Vital were contracted and paid by Dechert LLP, on behalf of RAKIA.

122. Because of Defendants' successful and unlawful phishing campaign against Azima, Azima had confidential information publicly exposed, suffered harm to business relationships, and suffered misappropriation of numerous trade secrets.

123. Defendants, Del Rosso, and Vital engaged in this conspiracy pursuant to a common scheme of damaging Azima and tarnishing his reputation.

PRAYER FOR RELIEF

On the basis of the foregoing, and such evidence as Plaintiff will present at trial, Plaintiff requests the entry of judgment in his favor and against Defendants on all counts of the Complaint and the award of the following relief

1. Compensatory damages incurred by Plaintiffs as a result of the actions of Defendants, in an amount to be determined at trial.

2. Statutory damages, in an amount to be determined at trial, including treble damages.

3. A mandatory injunction requiring Defendants to remove and return of Plaintiff's data from any computers, servers, or websites.

4. A prohibitory injunction obligating Defendants to refrain in the future from committing tortious acts against Plaintiff.

5. Pre-judgment and post-judgment interest in the amounts and at the rates provided by law.

6. Costs and expenses, including reasonable attorney's fees, incurred by Plaintiff in this action and as a result of the actions of Defendants alleged herein.

7. Such other and further relief as the Court deems just and proper.

JURY DEMAND

Plaintiff Farhad Azima respectfully requests a trial by jury of all issues so triable.

Dated: XXXX, 2020

Respectfully submitted,

/s/ Kirby D. Behre

Kirby D. Behre ()
Brian Hill ()
Tim O'Toole ()
Ian Herbert ()
Calvin Lee ()
Miller & Chevalier Chartered
900 16th Street, NW
Washington, D.C. 20006
Telephone: (202) 626-5800
Fax: (202) 626-5801
Email: kbehre@milchev.com

WOMBLE BOND DICKINSON (US) LLP

Christopher W. Jones
North Carolina Bar No. 27625

Ripley Rand
North Carolina Bar No. 22275
555 Fayetteville Street, Suite 1100
Raleigh, North Carolina 27601
Phone: 919-755-2100
Fax: 919-755-2150
Email: chris.jones@wbd-us.com
ripley.rand@wbd-us.com

Exhibit 2

(Witness Statement of Ian Herbert)

Filed on behalf of: Counterclaimant / Applicant
Witness: Ian A. Herbert
Number: 1
20 July 2023
Exhibit IAH1

IN THE HIGH COURT OF JUSTICE **Case No. HC-2016-002798**
BUSINESS AND PROPERTY COURTS
OF ENGLAND AND WALES
BUSINESS LIST (ChD)

Assigned to: THE HON MR JUSTICE MICHAEL GREEN

BETWEEN:

RAS AL KHAIMAH INVESTMENT AUTHORITY
Claimant and Defendant to Counterclaim

-and-

FARHAD AZIMA
Defendant, Counterclaimant and Applicant

-and-

DAVID NEIL GERRARD
Second Additional Defendant to Counterclaim

-and-

DECHERT LLP
Third Additional Defendant to Counterclaim

-and-

JAMES EDWARD DENISTON BUCHANAN
Fourth Additional Defendant to Counterclaim

-and-

STOKOE PARTNERSHIP SOLICITORS
Respondent

WITNESS STATEMENT OF IAN A. HERBERT

I, **Ian A. Herbert**, of Miller & Chevalier Chartered, of 900 16th Street NW, Black Lives Matter Plaza, Washington, D.C. 20006, United States of America, **SAY AS FOLLOWS**:

1. I am counsel at Miller & Chevalier Chartered in Washington, D.C., and I am part of the team that represents Farhad Azima in the United States.

2. The facts and matters set out in this statement are within my own knowledge unless otherwise stated, and I believe them to be true. Where I refer to information supplied by others, the source of the information is identified; facts and matters derived from other sources are true to the best of my knowledge and belief.

3. There is now produced and shown to me a document marked "Exhibit IAH1" to which reference will be made in the course of this statement in the form '[**IAH1/[page number**]'.

4. I make this statement in support of Farhad Azima in connection with his application for a third-party disclosure order against Stokoe Partnership Solicitors ("**Stokoe**") in respect of a laptop Mr Nicholas Del Rosso seeks an order in respect of. Below I describe information provided to me and my firm by CyberRoot Group ("**CyberRoot**") concerning Mr. Del Rosso.

5. Beginning in February 2023, CyberRoot, through its director Vijay Bisht, repeatedly contacted Farhad Azima's counsel at Miller & Chevalier ("**M&C**"), Kirby Behre, through the text messaging application Signal, seeking to provide evidence Mr. Bisht said supported Mr. Azima's case against Vital Management Services and Nicholas Del Rosso concerning the hacking of Mr. Azima. When asked for details about the information CyberRoot wished to share, Mr. Bisht repeatedly insisted upon an in-person meeting to provide CyberRoot's information. Mr. Azima's counsel declined to meet in person without CyberRoot first indicating what they were prepared to admit to and what documentary evidence they hold. M&C also asked what CyberRoot hoped to get out of an in-person meeting, and they refused to say.

6. Mr. Bisht on behalf of CyberRoot eventually agreed to provide a preview of the evidence CyberRoot possessed. In May 2023, CyberRoot asked M&C to communicate on a messaging application called "Twinme," a secure and encrypted end-to-end application for (among other things) text messages. CyberRoot then sent M&C a series of text messages on Twinme in which CyberRoot admitted to working with Mr. Del Rosso and others to

successfully phish and hack Mr. Azima and others starting in 2016. Attached as Exhibit 1 is a true and correct copy of those text messages as received **[IAH1/2-5]**.

7. Specifically, in the text messages, Mr. Bisht, on behalf of CyberRoot, admitted that:

7.1. Mr. Del Rosso first contacted CyberRoot in 2015 and asked CyberRoot to hack Mr. Azima.

7.2. CyberRoot successfully hacked Mr. Azima and others beginning in 2016.

7.3. After obtaining Mr. Azima's data by hack, CyberRoot sent that data to Mr. Del Rosso via WeTransfer links via encrypted messaging applications.

7.4. In June 2016, Mr. Del Rosso asked CyberRoot to transfer the hacked data onto laptops to be delivered to Mr. Neil Gerrard.

7.5. Mr. Gerrard instructed CyberRoot (through Mr. Del Rosso) to place the hacked data on the Internet, which CyberRoot did.

7.6. In 2017, at Mr. Del Rosso's instructions, CyberRoot delivered two mobile phones and one iPad to Mr. Del Rosso for secure communication.

7.7. Vikash Pandey would be willing to "reverse" his prior witness statement.

8. To prove that CyberRoot was behind the hacking that Mr. Del Rosso and Mr. Gerrard ordered, the Twinme text messages from Mr. Bisht also included the passwords of Mr. Azima's that CyberRoot had used to hack Mr. Azima.

9. CyberRoot said that they could provide additional information and corroboration if M&C agreed to meet in person. CyberRoot refused to meet in the U.S. or Europe, and it was eventually agreed that the parties would meet in Tokyo, Japan.

10. Kirby Behre and I met with CyberRoot directors Mr. Bisht and Mr. Chiranshu Ahuja in person on June 20-21, 2023, in Tokyo. I recognized Mr. Ahuja from photos available on the Internet. Mr. Bisht and Mr. Ahuja claimed to be speaking for CyberRoot and the remaining director, Mr. Vibhor Sharma. At the meetings, CyberRoot again admitted to hacking Mr. Azima at the direction of Mr. Del Rosso, Mr. Gerrard, and others, starting in 2015. CyberRoot provided more detail beyond what was included in the May 2023 text

messages and presented some documentary support. For example, Mr. Bisht and Mr. Ahuja admitted that:

10.1. Mr. Del Rosso continued to ask CyberRoot to attempt to target Mr. Azima and others as late as 2020, and CyberRoot did so.

10.2. Mr. Del Rosso requested that CyberRoot attempt to hack Mr. Azima in 2019 to assist Mr. Gerrard in an upcoming trial involving Mr. Azima, and CyberRoot did so.

10.3. Mr. Del Rosso requested CyberRoot target the email addresses of others, such as cameron@riskprofiling.co.uk during 2018, and CyberRoot did so.

10.4. Mr. Del Rosso and Mr. Gerrard instructed CyberRoot to publish Mr. Azima's stolen data on the Internet, first in 2016 and then again in 2018 and 2019, which CyberRoot did.

10.5. In 2017, Mr. Del Rosso stopped paying CyberRoot through Vital Management Services because he was worried about the payments being traced back to him. He used multiple other entities to make payments to CyberRoot, totalling more than $2.3 million.

10.6. After Mr. Azima sued Mr. Del Rosso in the United States in October 2020, Mr. Del Rosso instructed CyberRoot to destroy all documents, but CyberRoot did not do so.

10.7. After this lawsuit was filed, Mr. Del Rosso's lawyers, including Brandon Neuman and Jeffrey Kelly, pressured Mr. Bisht and Mr. Vikash Pandey to sign false statements denying the hacking of Mr. Azima.

11. After CyberRoot's presentation admitting to hacking and related illegal activity, CyberRoot for the first time explained what it was seeking. CyberRoot said that it wished to be paid $20 million in exchange for documentation backing up the information they had already provided. We rejected it as not being a serious request. CyberRoot also requested "immunity."

12. This week, Mr. Bisht used the settings within Signal and Twinme to delete text messages, including the admissions attached to this statement. Mr. Bisht changed the settings on Signal to delete messages after 24 hours and deleted portions of the text messages on

Twinme attached to this statement, specifically those in which he confessed that CyberRoot hacked Mr. Azima. I therefore prepared this witness statement.

STATEMENT OF TRUTH

I believe that the facts stated in this witness statement are true. I understand that proceedings for contempt of court may be brought against anyone who makes, or causes to be made, a false statement in a document verified by a statement of truth without an honest belief in its truth.

Ian Herbert
.....

IAN A. HERBERT

Dated: 20 July 2023

Case No. HC-2016-002798

IN THE HIGH COURT OF JUSTICE

BUSINESS AND PROPERTY COURTS OF ENGLAND AND WALES

BUSINESS LIST (ChD)

RAS AL KHAIMAH INVESTMENT AUTHORITY

Claimant and Defendant to Counterclaim

-and-

FARHAD AZIMA

Defendant, Counterclaimant and Applicant

-and-

DECHERT LLP

Third Additional Defendant to Counterclaim

-and-

JAMES EDWARD DENISTON BUCHANAN

Fourth Additional Defendant to Counterclaim

-and-

STOKOE PARTNERSHIP SOLICITORS

Respondent

Burlingtons Legal LLP

5 Stratford Place

London W1C 1AX

Ref: DPH25/AZI.3/2

Solicitors for the Defendant, Counterclaimant and Applicant

Exhibit 3
(Exhibit to Herbert Witness Statement)

Claim no. HC-2016-002798

B E T W E E N:

RAS AL KHAIMAH INVESTMENT AUTHORITY
Claimant and Defendant to Counterclaim

-and-
FARHAD AZIMA
Defendant and Counterclaimant

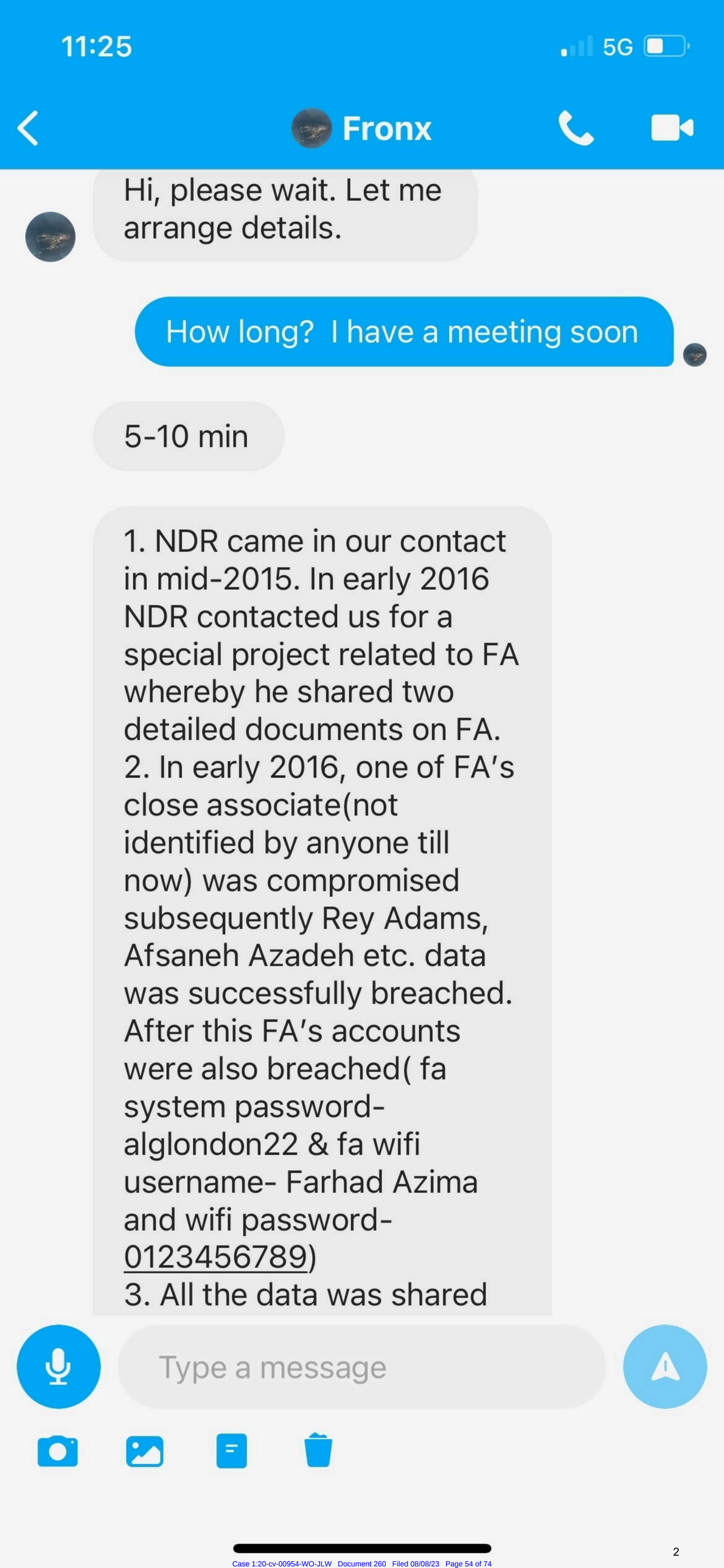
~~**-and-**~~
~~**STUART ROBERT PAGE**~~
~~**First Additional Defendant to Counterclaim**~~

-and-
DAVID NEIL GERRARD
Second Additional Defendant to Counterclaim

-and-
DECHERT LLP
Third Additional Defendant to Counterclaim

-and-
JAMES EDWARD DENNISTON BUCHANAN
Fourth Additional Defendant to Counterclaim

EXHIBIT IAH1


11:25
5G
Fronx
Hi, please wait. Let me arrange details.
How long? I have a meeting soon
5-10 min
1. NDR came in our contact in mid-2015. In early 2016 NDR contacted us for a special project related to FA whereby he shared two detailed documents on FA.
2. In early 2016, one of FA's close associate(not identified by anyone till now) was compromised subsequently Rey Adams, Afsaneh Azadeh etc. data was successfully breached. After this FA's accounts were also breached(fa system password- alglondon22 & fa wifi username- Farhad Azima and wifi password- 0123456789)
3. All the data was shared
Type a message

with NDR through we transfer links via an encrypted communication app.
Further updates of data for Rey and FA were shared with NDR.
4. On instructions of NDR in June 2016; three laptops were arranged and all the breached data was copied into them. These laptops were delivered in London to Neil Gerrard via special route.
5. Around July 2016, based on detailed discussion between NDR, Neil and others it was considered to use the data of FA in court and for this purpose data had to be put on Internet securely without traces.
6. FA data was divided into 3 tranches and was put on torrents and we-transfer in multiple phases as instructed by Neil via NDR.
7. In 2017, two mobile phones and one ipad were

instructed by Neil via NDR.
7. In 2017, two mobile phones and one ipad were specifically crafted and delivered to NDR in Dubai on his instructions.
8. In late 2017, number of meeting were held in RAK. Multiple meetings were held in London and Dubai in 2017, 2018 and so on.

This is just a small writeup, everything in detail and what transpired from 2018 till now can be discussed later on physically.

Also, Pandey can assist in reversing his 2 witness statement and assist further if needed.

18 May 4:07 AM

Hi, I hope our intent is clear to you now.
Let me know if we can proceed further on this?

Type a message

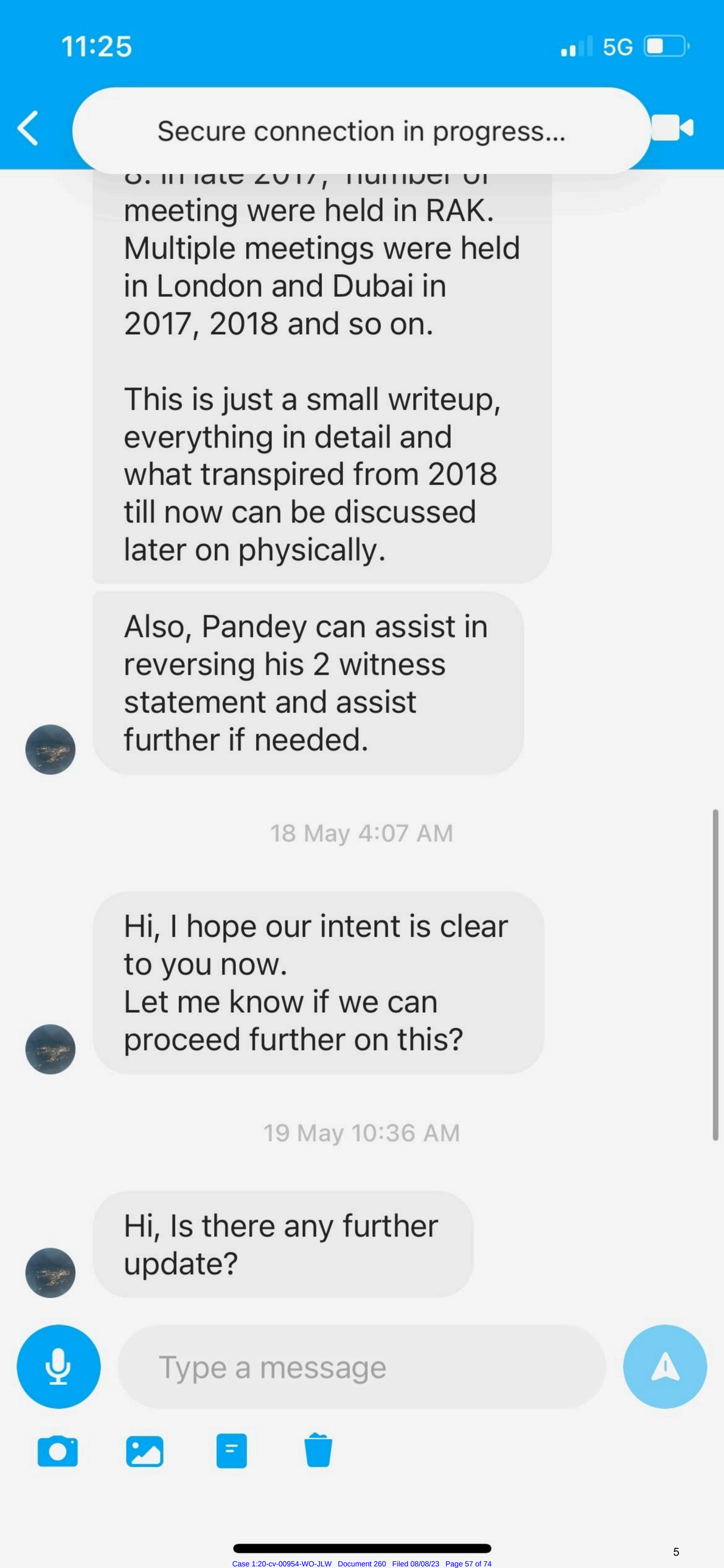

11:25
5G
Secure connection in progress...
meeting were held in RAK. Multiple meetings were held in London and Dubai in 2017, 2018 and so on.
This is just a small writeup, everything in detail and what transpired from 2018 till now can be discussed later on physically.
Also, Pandey can assist in reversing his 2 witness statement and assist further if needed.
18 May 4:07 AM
Hi, I hope our intent is clear to you now.
Let me know if we can proceed further on this?
19 May 10:36 AM
Hi, Is there any further update?
Type a message

Exhibit 4
(Declaration of Ian Herbert)

UNITED STATES DISTRICT COURT
FOR THE MIDDLE DISTRICT OF NORTH CAROLINA
CASE NO. 20-cv-954-WO-JLW

FARHAD AZIMA, Plaintiff, v. NICHOLAS DEL ROSSO and VITAL MANAGEMENT SERVICES, INC., Defendants.	**DECLARATION OF IAN A. HERBERT IN SUPPORT OF PLAINTIFF'S SUPPLEMENT TO HIS MOTIONS TO COMPEL PRODUCTION OF DOCUMENTS (ECF No. 130) AND FURTHER DEPOSITION TESTIMONY (ECF No. 188)**

I, Ian A. Herbert**,** pursuant to 28 U.S.C. § 1746, do hereby declare under penalty of perjury the following:

1. I am counsel at the law firm of Miller & Chevalier Chartered, 900 16th Street NW, Washington, D.C., 20036. I am a member in good standing of the bar of the District of Columbia Bar and I have made a special appearance in this Court on behalf of Plaintiff Farhad Azima. ECF No. 19.

2. Recently, CyberRoot Group ("**CyberRoot**") has provided to me and my firm information concerning this matter. I have included in this declaration the information that is most relevant to Mr. Azima's Supplement to Plaintiff's Motion to Compel, but not all information provided by CyberRoot.

3. Beginning in February 2023, CyberRoot, through its director Vijay Bisht, repeatedly contacted Farhad Azima's counsel at Miller & Chevalier

("**M&C**"), Kirby Behre, through the text messaging application Signal, seeking to provide evidence Mr. Bisht said supported Mr. Azima's case against Vital Management Services and Nicholas Del Rosso concerning the hacking of Mr. Azima. When asked for details about the information CyberRoot wished to share, Mr. Bisht repeatedly insisted upon an in-person meeting to provide CyberRoot's information. Mr. Azima's counsel declined to meet in person without CyberRoot first indicating what they were prepared to admit to and what documentary evidence they hold. M&C also asked what CyberRoot hoped to get out of an in-person meeting, and they refused to say.

4. Mr. Bisht on behalf of CyberRoot eventually agreed to provide a preview of the evidence CyberRoot possessed. In May 2023, CyberRoot asked M&C to communicate on a messaging application called "Twinme," a secure and encrypted end-to-end application for (among other things) text messages. CyberRoot then sent M&C a series of text messages on Twinme in which CyberRoot admitted to working with Mr. Del Rosso and others to successfully phish and hack Mr. Azima and others starting in 2016. Attached as Exhibit A is a true and correct copy of those text messages as received.

5. Specifically, in the text messages, Mr. Bisht, on behalf of CyberRoot, admitted that:

a. Mr. Del Rosso first contacted CyberRoot in 2015 and asked CyberRoot to hack Mr. Azima.

b. CyberRoot successfully hacked Mr. Azima and others beginning in 2016.

c. After obtaining Mr. Azima's data by hack, CyberRoot sent that data to Mr. Del Rosso via WeTransfer links via encrypted messaging applications.

d. In June 2016, Mr. Del Rosso asked CyberRoot to transfer the hacked data onto laptops to be delivered to Mr. Neil Gerrard.

e. Mr. Gerrard instructed CyberRoot (through Mr. Del Rosso) to place the hacked data on the Internet, which CyberRoot did.

f. In 2017, at Mr. Del Rosso's instructions, CyberRoot delivered two mobile phones and one iPad to Mr. Del Rosso for secure communication.

g. Vikash Pandey would be willing to "reverse" his prior witness statement.

6. To prove that CyberRoot was behind the hacking that Mr. Del Rosso and Mr. Gerrard ordered, the Twinme text messages from Mr. Bisht also included the passwords of Mr. Azima's that CyberRoot had used to hack Mr. Azima.

7. CyberRoot said that they could provide additional information and corroboration if M&C agreed to meet in person. CyberRoot refused to

meet in the U.S. or Europe, and it was eventually agreed that the parties would meet in Tokyo, Japan.

8. Kirby Behre and I met with CyberRoot directors Mr. Bisht and Mr. Chiranshu Ahuja in person on June 20-21, 2023, in Tokyo. I recognized Mr. Ahuja from photos available on the Internet. Mr. Bisht and Mr. Ahuja claimed to be speaking for CyberRoot and the remaining director, Mr. Vibhor Sharma. At the meetings, CyberRoot again admitted to hacking Mr. Azima at the direction of Mr. Del Rosso, Mr. Gerrard, and others, starting in 2015. CyberRoot provided more detail beyond what was included in the May 2023 text messages and presented some documentary support. For example, Mr. Bisht and Mr. Ahuja admitted that:

   a. Mr. Del Rosso continued to ask CyberRoot to attempt to target Mr. Azima and others as late as 2020, and CyberRoot did so.

   b. Mr. Del Rosso requested that CyberRoot attempt to hack Mr. Azima in 2019 to assist Mr. Gerrard in an upcoming trial involving Mr. Azima, and CyberRoot did so.

   c. Mr. Del Rosso requested CyberRoot target the email addresses of others, such as cameron@riskprofiling.co.uk during 2018, and CyberRoot did so.

d. Mr. Del Rosso and Mr. Gerrard instructed CyberRoot to publish Mr. Azima's stolen data on the Internet, first in 2016 and then again in 2018 and 2019, which CyberRoot did.

e. In 2017, Mr. Del Rosso stopped paying CyberRoot through Vital Management Services because he was worried about the payments being traced back to him. He used multiple other entities to make payments to CyberRoot, totalling more than $2.3 million.

f. After Mr. Azima sued Mr. Del Rosso in this proceeding in October 2020, Mr. Del Rosso instructed CyberRoot to destroy all documents, but CyberRoot did not do so.

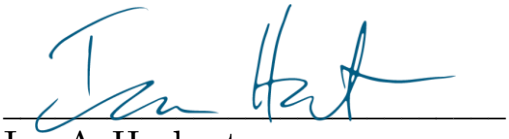
g. After this lawsuit was filed, Mr. Del Rosso's lawyers, including Brandon Neuman and Jeffrey Kelly, pressured Mr. Bisht and Mr. Vikash Pandey to sign false statements denying the hacking of Mr. Azima.

9. After CyberRoot's presentation admitting to hacking and related illegal activity, CyberRoot for the first time explained what it was seeking. CyberRoot said that it wished to be paid $20 million in exchange for documentation backing up the information they had already provided. We rejected it as not being a serious request. CyberRoot also requested "immunity."

10. This week, Mr. Bisht used the settings within Signal and Twinme to delete text messages, including the admissions attached to this

statement. Mr. Bisht changed the settings on Signal to delete messages after 24 hours and deleted portions of the text messages on Twinme attached to this statement, specifically those in which he confessed that CyberRoot hacked Mr. Azima. I therefore prepared this witness statement.

I declare under penalty of perjury that the foregoing is true and correct. Executed on July 20, 2023, in Washington, D.C.



Ian A. Herbert

IN THE UNITED STATES DISTRICT COURT
FOR THE MIDDLE DISTRICT OF NORTH CAROLINA
CASE NO. 20-CV-954-WO-JLW

FARHAD AZIMA,

Plaintiff,

v.

NICHOLAS DEL ROSSO and VITAL MANAGEMENT SERVICES, INC.,

Defendants.

CERTIFICATE OF SERVICE

I hereby certify that I electronically filed the foregoing with the Clerk of Court using the CM/ECF system, which will send electronic notification of this Declaration to the following attorneys:

Brandon S. Neuman, Esq.
John Branch, III, Esq.
Jeffrey M. Kelly, Esq.
Nathaniel J. Pencook, Esq.
NELSON MULLINS RILEY & SCARBOROUGH, LLP
301 Hillsborough Street, Suite 1400
Raleigh, NC 27603
brandon.neuman@nelsonmullins.com
jeff.kelly@nelsonmullins.com
nate.pencook@nelsonmullins.com
john.branch@nelsonmullins.com
Tel.: 919.329.3800
Fax.: 919.329.3799

Samuel Rosenthal, Esq.
NELSON MULLINS RILEY & SCARBOROUGH LLP
101 Constitution Ave NW, Suite 900
Washington, DC 20001
Tel.: 202-689-2951
Fax: 202-689-2860
sam.rosenthal@nelsonmullins.com

Counsel for Defendants

This, the 20th day of July, 2023.

WOMBLE BOND DICKINSON (US) LLP

/s/ *Ripley Rand*
Ripley Rand
North Carolina State Bar No. 22275
555 Fayetteville Street, Suite 1100
Raleigh, NC 27601
Telephone: (919) 755-8125
Facsimile: (919) 755-6752
Email: ripley.rand@wbd-us.com

Counsel for Plaintiff

Exhibit A to Declaration of Ian A. Herbert

11:25 5G

Fronx

Hi, please wait. Let me arrange details.

How long? I have a meeting soon

5-10 min

1. NDR came in our contact in mid-2015. In early 2016 NDR contacted us for a special project related to FA whereby he shared two detailed documents on FA.
2. In early 2016, one of FA's close associate(not identified by anyone till now) was compromised subsequently Rey Adams, Afsaneh Azadeh etc. data was successfully breached. After this FA's accounts were also breached(fa system password- alglondon22 & fa wifi username- Farhad Azima and wifi password- 0123456789)
3. All the data was shared

Type a message

with NDR through we transfer links via an encrypted communication app.
Further updates of data for Rey and FA were shared with NDR.
4. On instructions of NDR in June 2016; three laptops were arranged and all the breached data was copied into them. These laptops were delivered in London to Neil Gerrard via special route.
5. Around July 2016, based on detailed discussion between NDR, Neil and others it was considered to use the data of FA in court and for this purpose data had to be put on Internet securely without traces.
6. FA data was divided into 3 tranches and was put on torrents and we-transfer in multiple phases as instructed by Neil via NDR.
7. In 2017, two mobile phones and one ipad were

instructed by Neil via NDR.
7. In 2017, two mobile phones and one ipad were specifically crafted and delivered to NDR in Dubai on his instructions.
8. In late 2017, number of meeting were held in RAK. Multiple meetings were held in London and Dubai in 2017, 2018 and so on.

This is just a small writeup, everything in detail and what transpired from 2018 till now can be discussed later on physically.

Also, Pandey can assist in reversing his 2 witness statement and assist further if needed.

18 May 4:07 AM

Hi, I hope our intent is clear to you now.
Let me know if we can proceed further on this?

Type a message

8. In late 2017, number of meeting were held in RAK. Multiple meetings were held in London and Dubai in 2017, 2018 and so on.

This is just a small writeup, everything in detail and what transpired from 2018 till now can be discussed later on physically.

Also, Pandey can assist in reversing his 2 witness statement and assist further if needed.

18 May 4:07 AM

Hi, I hope our intent is clear to you now.
Let me know if we can proceed further on this?

19 May 10:36 AM

Hi, Is there any further update?

Type a message

Exhibit 5
(Vijay Bisht Grocery Receipt)

Original Tax Invoice

Details of Supplier

Innovative Retail Concepts Pvt Ltd,Innovative Retail Concepts Pvt Ltd,Khasra No- 1892/1, Shyam Chowk,, Sector-52, village , 122003,Gurgaon,06,122003, Haryana (06)
Tel.: 1860 123 1000
GSTIN : 06AACCI2053A1ZB
CIN: U74130KA2010PTC052192
FSSAI Lic. No: 10820005000102

Bill to/Ship to:

vijay bisht[redacted],Gurgaon,06,122011, Haryana (06)

Invoice Number	IEXHR23IUAB51722
Invoice Date	21/06/2023

We appreciate your concern towards the environment. In line with this we request you to please keep aside the fruits and vegetables tray packs, so that we can collect them back next time we visit your place.

Additional Information

Order No	EXN-1242231943-20230620
Slot	Wed 21 Jun 2023 between 08:00 AM and 10:00 AM
Payable Amount	Rs.0.00
Payment Mode	CARD
Source	bb-b2c
No. of Items	8

Sl No.	Item Description	HSN Code	Quantity	Unit Price*	Unit Tax Value	Gross Value*	Discount/ Margin*	Delivery Charge	Taxable Value	CGST Rate(%) Amount	SGST/ UTGST% Rate(%) Amount	CESS Amount	TOTAL Value
1	MAGGI Nutri-Licious Masala Veg Atta Noodles - Herbs & Spice Blend, Iron & Fibre Rich 290 g Pouch	19024090	1.00	102.00	82.14	102.00	10.00	0.00	82.14	6.0% 4.93	6.0% 4.93	0.0	92.00
2	Lijjat Papad - Moong 250 g	19051000	1.00	84.00	84.00	84.00	0.00	0.00	84.00	0.0% 0.0	0.0% 0.0	0.0	84.00
3	BB Royal Organic - Mixed Dal 1 kg	09096230	1.00	200.00	152.38	200.00	40.00	0.00	152.38	2.5% 3.81	2.5% 3.81	0.0	160.00
4	ROYAL Premium Plain Chana - Without Skin, Healthy Snack 200 g	21069060	1.00	60.00	57.14	60.00	0.00	0.00	57.14	2.5% 1.43	2.5% 1.43	0.0	60.00
5	MAXI Zoom Car Junior Toothbrush - Soft Bristles, Comfortable Grip 2 pcs (Buy 1 Get 1 Free)	96032100	1.00	75.00	63.56	75.00	0.00	0.00	63.56	9.0% 5.72	9.0% 5.72	0.0	75.00

6	Colgate Kids Toothpaste - 2-5 Years, Strawberry Flavour 40 g	33061020	1.00	68.00	57.63	68.00	0.00	0.00	57.63	9.0% 5.19	9.0% 5.19	0.0	68.00
7	ALPENLIEBE Juzt Jelly - With 25% Fruit Pulp, Assorted Flavour, Cars & Planes 71.5 g Pouch	17049030	1.00	30.00	26.79	30.00	0.00	0.00	26.79	6.0% 1.61	6.0% 1.61	0.0	30.00
8	Fackelmann Multi-Purpose Wooden Toothpicks, 6.5 Cm, Set of 190 190 pcs	44199090	1.00	99.00	61.61	99.00	30.00	0.00	61.61	6.0% 3.7	6.0% 3.7	0.0	69.00
								0.00	585.22				638.00

GST Information

CGST%	Sale	Taxable Value	Tax Value
6.0%	Rs.191.00	Rs.170.54	Rs.10.24
2.5%	Rs.220.00	Rs.209.52	Rs.5.24
9.0%	Rs.143.00	Rs.121.19	Rs.10.91

SGST%	Sale	Taxable Value	Tax Value
6.0%	Rs.191.00	Rs.170.54	Rs.10.24
2.5%	Rs.220.00	Rs.209.52	Rs.5.24
9.0%	Rs.143.00	Rs.121.19	Rs.10.91

Sub Total	Rs.638.00
Credit availed from bigbasket Wallet	Rs.0.00
Redeemed Neucoins	0.0
Final Total	Rs.638.00

You Saved: **Rs.80.00**

Total Invoice value (In Figure): **Rs.638.00**

Total Invoice value (In words): **Rs.Six Hundred Thirty Eight Rupees**

*Includes GST component

As per Section 31 of CGST Act read with Rules, invoice is issued at the point of delivering the goods

Disclaimer: The final invoice copy will be available on the app under order details page.